

South Carolina

Enterprise Architecture

Security Domain

Hardware Sanitization Policy

v1.0 - August 23, 2006



Table of Contents

Table of Contents.....	2
1.0 Introduction.....	3
1.1 Authority	3
1.2 Purpose.....	4
1.3 Scope	4
1.4 Background	4
1.5 Definitions	4
2.0 Policy.....	6
2.1 Preface	6
2.2 Disposal Scenarios.....	6
2.3 Technical Guidance on Sanitization	7
2.4 Non-Compliance	7
2.5 Environmental Guidance.....	7
2.6 Software Licensing	7
2.7 Surplused Items.....	8
2.8 Retention Period.....	8
2.9 Training	8
Appendix A - Suggested South Carolina Sanitization Form.....	9
Appendix B - Suggested South Carolina Sanitization Schedule	10
Appendix C - Surplus Property Turn-In Document (TID).....	11
Appendix D - Sample Designee Form.....	12

1.0 Introduction

1.1 Authority

The State Budget and Control Board is authorized to undertake the development of enterprise architecture policies and standards as set forth in **Section 11-35-1580** of the *South Carolina Consolidated Procurement Code*. This Section states, in part, that the State Budget and Control Board shall be responsible for:

- a. Assessing the need for and use of information technology;
- b. Administering all procurement and contracting activities undertaken for governmental bodies involving information technology in accordance with this chapter;
- c. Providing for the disposal of all information technology property surplus to the needs of a using agency;
- d. Evaluating the use and management of information technology;
- e. Operating a comprehensive inventory and accounting reporting system for information technology;
- f. Developing policies and standards for the management of information technology in state government;
- g. Initiating a state plan for the management and use of information technology;
- h. Providing management and technical assistance to state agencies in using information technology; and
- i. Establishing a referral service for state agencies seeking technical assistance or information technology services.

The State Budget and Control Board has delegated this authority to the Division of the State CIO. Based upon this authority, the Division of the State CIO has established the SC Enterprise Architecture to conduct operations and take actions to fulfill this mandate.

In addition, South Carolina's Code of Laws, **Section 1-11-435** *Protection of Critical Information Technology Infrastructure and Data Systems*, states in part, that "the Office of the State Chief Information Officer (CIO) should develop a Critical Information Technology Infrastructure Protection Plan devising policies and procedures to provide for the confidentiality, integrity, and availability of [...] critical data and information systems.

1.2 Purpose

The purpose of this policy is to protect the intellectual property of South Carolina and the confidentiality of its employees, partners and citizens. It defines the data sanitization standards and procedures to be used in the pre-disposal of State hardware.

1.3 Scope

This policy applies to all hardware owned or leased by the State of South Carolina that is capable of storing intellectual property or personal information related to the privacy of its employees, partners and citizens. Such devices include, but are not limited to, the following:

- ✓ Portable and notebook computers
- ✓ Workstations
- ✓ Servers, routers and switches
- ✓ Mobile devices, such as PDAs and smart phones
- ✓ Removable storage media, such as flash memory devices, floppy disk, optical CD and DVD media, tape and other long-term storage media

1.4 Background

As our society has become increasingly dependant on information systems, the risks associated with an attacker gaining access to sensitive data has equally increased. In response, organizations have instituted a wide variety of sophisticated deterrents designed to keep assailants at bay. As a result, attackers have been forced to look outside the system for information. One popular method of attack is to recover residual data from discarded media. Once recovered, the attack exposes an organization to potential negative consequences, including regulatory fines (e.g., HIPAA) and punitive awards. Therefore, it is imperative that all State organizations follow a policy to ensure the protection of sensitive data both inside and outside the organization.

1.5 Definitions

Authorization: The granting of rights, which includes the granting of access based on an authenticated identity.

Break in Service: A significant period of time in which a specific piece of hardware will not be utilized.

CIO: Chief Information Officer.

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Data: Any information created, stored (temporarily or permanently) electronically, regardless of the media type. Data may include, but is not limited to personal information, reports, files, images, communications, etc.

Designee: An agency employee of sufficient rank who has been formerly empowered to fulfill a specific purpose, office, or duty by the agency director (see Appendix D - *Sample Designee Form*).

HIPAA: The Health Insurance Portability and Accountability Act creates a standard for healthcare providers and institutions to protect the confidentiality and integrity of personal health information.

Personal Information: Any of the following elements: social security number, driver license number, account number, credit or debit card number, security code, access code, password, etc.

Procedures: Specific operational steps defined by agencies that individuals must follow in order to achieve agency goals.

Privacy: The right of an individual or organization to control the collection, storage, and dissemination of information about themselves.

Sanitization: The process of erasing or destroying electronic data from information technology resources and associated storage media in a manner that provides reasonable assurance that the information cannot be removed.

State: The State of South Carolina.

Statute of Limitations: Is a formal law within the legal system that establishes the maximum period of time that legal proceedings may be initiated.

System: An interconnected set of information resources under the same direct management control that shares common functionality. A system may include hardware, software, data, applications and/or telecommunications infrastructure.

Third-Party: Any non-state entity employees such as a contractor, vendor, consultant, etc.

User: Any State employee, third-party contractor or any other individual who is authorized to access a State system for a legitimate government purpose.

2.0 Policy

2.1 Preface

All equipment that may contain intellectual property or personal information must be sanitized as outlined in this policy prior to transfer for other uses or for disposal. Compliance with this policy is mandatory.

In general, always consult with your IT department prior to disposing of any computer equipment. They can assist in the proper sanitization of any equipment. Specifically, agency directors or their designee must complete and sign a certification that the hardware has been properly sanitized before it can be surplused, transferred, inventoried due to a break in service, donated or junked. Copies of all certification statements must be maintained by local IT staff and provided to the State's Surplus Property Manager when appropriate (see *Surplused Items* section). A sample certification form is provided in Appendix A.

2.2 Disposal Scenarios

South Carolina recognizes two categories for disposing of hardware:

1. Hardware Transferred Internally

Hardware may not require sanitization when transferred to another user within the same department. Hardware that is either transferred to a different department or outside its current roles and responsibilities must be sanitized as specified in the *Hardware Transferred Externally* section of this document.

2. Hardware Transferred Externally

All hardware transferred externally must be sanitized according to the methods defined in the *Technical Guidance on Sanitization* section of this policy. This scenario includes, but is not limited to the following:

- Hardware transferred to the private ownership of employees
- Hardware transferred to charitable organizations
- Hardware returned to a lessor
- Hardware returned to a vendor for servicing or maintenance
- Hardware released to a third-party for disposal

2.3 Technical Guidance on Sanitization

South Carolina recognizes two primary methods for the sanitization of hardware.

1. Physical Destruction

Hardware may be sanitized by crushing, shredding, incineration, or smelting.

2. Digital Sanitization

Deleting files is insufficient to sanitize hardware. Therefore, a digital sanitization tool must be used. The tool must conform to the Department of Defense's *DoD 5220.22-M* specifications, available at <http://www.dss.mil/files/pdf/nispom2006-5220.pdf>. Current examples of such tools include: OnTrack DataEraser, Infracore Sanitizer, White Canyon SecureClean, Norton WipeInfo, and PowerQuest DataGone.

In addition, sanitization methods must follow the recommendations outlined in the National Institute of Standards and Technology's *Special Publication 800-88 - Guidelines for Media Sanitization*, available at http://csrc.nist.gov/publications/nistpubs/800-88/SP800-88_Aug2006.pdf.

2.4 Non-Compliance

Non-compliance must be reported immediately to the organization's Manager or Director for the appropriate remedial action as defined in the agency's progressive discipline policy. Each agency is responsible for establishing and including the appropriate response(s) within their internal progressive discipline policy.

Any agency not adhering to this policy may potentially expose itself to lawsuits and regulatory fines to include possible punitive damages.

2.5 Environmental Guidance

Agencies must adhere to the regulations detailed on the Environmental Protection Agency's (EPA) *eCycling* website (www.epa.gov/e-cycling) and any applicable State laws when disposing of computer equipment. For example, by law, the State's Surplus Property Manager must approve any items before they can be junked.

2.6 Software Licensing

In general, most software vendors (e.g., Microsoft®) do not allow ad hoc licensing transfers to third-parties and require adherence to strict relicensing procedures in order to do so. Agencies should consult their original licensing agreement to determine the legality of any licensing issues. If an agency can

not explicitly determine the right to relicensing, then the software in questions, including operating systems, should be removed prior to disposal.

2.7 Surplused Items

By law, all State owned property must be disposed of through the State's Surplus Property Manager (<http://www.gs.sc.gov/surplus/SP-index.phtml> or 803-896-6880). Any computer related hardware must be sanitized in accordance with this policy and be documented as such in conjunction with the *Surplus Property Turn-In Document* or TID (see Appendix C).

State Agencies are strongly encouraged to surplus items instead of junking them as a cost effective and environmentally friendly alternative. For example, a typical PC contains pounds of toxic waste such as lead. Improper disposal could result in regulatory fines and environmental damage. Moreover, many suppliers have take-back programs, but usually charge for such services. Conversely, the State's Surplus Property Office charges a small handling fee but will refund any additional monies collected at sale to the donating agency. Agencies are encouraged to leave equipment intact (including software) as much as possible in order to maximize resale value, so long as it does not conflict with any licensing (see the *Software Licensing* section) agreements or sanitization standards in this policy.

2.8 Retention Period

Agencies should retain copies of their sanitization forms for a three (3) year period.

2.9 Training

Each State Agency is responsible for ensuring that its employees are properly trained in accordance with this policy and any related internal agency policies and procedures.

Appendix A - Suggested South Carolina Sanitization Form**South Carolina Sanitization Form**

=====

Agency Control Number: _____

State Agency: _____

Item Description: _____

Serial: _____

Sanitization Method Used: _____

Final Disposition:

? Disposed

? Reused Internally

? Sent to Surplus Property

? Returned to Manufacturer

? Other: _____

Sanitization:

Date Conducted: _____

By (Print Name): _____

Phone Number: _____

Signature: _____

Appendix B - Suggested South Carolina Sanitization Schedule

South Carolina Sanitization Form Certification: Removal of Data and Software

Agency Name: _____	Control Number: _____	Page _____ of _____
--------------------	-----------------------	---------------------

Item # (A)	Description (B)	Serial Number (C)	Sanitization Method (D)	Signature * (E)	Date (F)	Status Code (G)
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						

* I certify that all data and licensed software have been removed from this computer.

(Rev 08/06)

Status codes: 1 - Disposed, 2 - Reused Internally, 3 - Sent to Surplus Property (record Surplus TID #), 4 - Returned to Manufacturer, 5 - Other (specify)

Appendix C - Surplus Property Turn-In Document (TID)

Form No. 1 (Rev 10/87)

TURN-IN DOCUMENT (TID) SURPLUS PROPERTY

TO: SURPLUS PROPERTY OFFICE
1441 BOSTON AVENUE
WEST COLUMBIA, SC 29169

PAGE ___ of ___

SPO USE ONLY	
SPO CONTROL # _____	
DATE SCHEDULED FOR PICKUP OR DELIVERY _____	

1. DATE MAILED <u>12/25/01</u>	2. AGENCY REPORT NO. _____	3. TOTAL A/C COST \$ _____
4. FROM AGENCY NO. _____	NAME: _____	ADDRESS: _____
CITY, STATE AND ZIP CODE _____		TELEPHONE NUMBER _____
5. REIMBURSEMENT REQ. <input type="checkbox"/> YES <input type="checkbox"/> NO	FUND CODE TO BE REIMBURSED (IF ANY) _____	
6. AGENCY CONTACT PERSON: NAME _____	ADDRESS: _____	TELEPHONE NUMBER _____
CITY, STATE AND ZIP CODE _____		SIGNATURE _____
7. REPORT APPROVED BY: NAME _____	TITLE _____	
8. DATE REQUESTED FOR DELIVERY OR PICKUP: _____	9. LOCATION OF PROPERTY _____	
10. RELEASED BY SIGNATURE (AGENCY) _____	DATE _____	11. SCREENED BY: _____
12. RECEIVED AT SPO: SIGNATURE _____	DATE _____	CYCLE NO. _____
13. SURPLUS PROPERTY LISTINGS:		

ITEM NUMBER (A)	COMMODITY CODE (B)	YEAR PURCHASED (C)	DESCRIPTION (D)	DECAL NUMBER (E)	QUANTITY (F)	UNIT OF MEASURE (G)	ACQUISITION COST		SPO USE ONLY COND. SERVICE CHG. S OR J (IF APP.)	
							PER UNIT (H)	TOTAL (I)		
1									(J)	(K)
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										
17										
18										
19										
20										
21										
22										
23										
24										
25										
26										

Appendix D - Sample Designee Form**Agency Name**

Street Address
City, State Zip Code
Phone ? Fax Number

DESIGNEE FORM

I, _____, certify that the following person(s)
(Print: Name of Agency Director)

is authorized to sign, on my behalf, attesting to this agency's adherence to
the State's Hardware Sanitization Policy.

Designee Name*

Designee Title

Designee Signature

_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

* Designee must be trained on the policies and procedures.

Director Name: _____

Director Signature: _____

Date Signed: _____